Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for processing an access-request message for packet service, comprising:

writing a temporary randomly generated authenticator value in an attribute field of an access-request message;

encrypting a user password using the temporary authenticator value;

executing an encryption algorithm using the access-request message having the temporary authenticator value and the encrypted user password to generate a message digest, the access-request message having an authenticator field that is filled with a prescribed value;

generating a final access-request message, the final access-request message being generated by using the access-request message and replacing the value of the authenticator field with the message digest;

transmitting the final access-request message to an Authentication, Authorization and Accounting (AAA) server; and

verifying the final access-request message by the AAA server using the prescribed ~~value~~value,

wherein the prescribed value is a value previously defined between a foreign agent and the AAA server.

2. (Canceled)

3. (Currently Amended) The method of claim 1, wherein verifying the final access-request message comprises:

temporarily storing the value of the authenticator field of the final access-request message;

filling the authenticator field with the prescribed value;

performing an encrypting algorithm to obtain a second message digest; and

verifying the access-request message by comparing the temporarily stored value of the authenticator field to the second message digest.

4. (Currently Amended) The method of claim 3, wherein verifying the final access-request message further comprises:

determining the final access-request message to be normal if the temporarily stored authenticator value and the second message digest are identical to each other; and

determining the final access-request message to be abnormal if the temporarily stored authenticator value and the second message digest are not identical to each other.

5. (Currently Amended) The method of claim 4, further comprising:

processing the final access-request message if the final access-request message is normal; and

performing a user authentication by decrypting the encrypted user password written in the attribute field of the processed final access-request message.

6. (Currently Amended) The method of claim 5, wherein performing the user authentication comprises:

decrypting the encrypted user password written in the attribute field of the final access-request message using the temporary authenticator value of the final access-request message;

comparing the decrypted user password with the user password stored in a data base;

determining the user authentication to be successful if the decrypted user password and the stored user password are identical to each other; and

determining the user authentication to have failed if the decrypted user password and the stored user password are not identical to each other.

7. (Currently Amended) The method of claim 4, further comprising discarding the final access-request message if the final access-request message is determined to be abnormal.

8. (Currently Amended) The method of claim 1, wherein the randomly generated authenticator value is ~~created differently~~ randomly generated every time a message is generated.

9. (Previously Presented) A method for processing an access-request message for a packet service in a communication system, comprising:

writing an authenticator value for authenticating an access-request message in an authenticator field of an access-request message and transmitting an access-request message;

verifying the access-request message by using the authenticator value of the access-request message when the access-request message is received;

processing the access-request message if the access-request message is successfully verified; and

performing user authentication by decrypting an encrypted user password of the processed access-request message using a temporary authenticator value of the processed

access-request message and a shared secret key that is known to each of a message transmitter and a message receiver.

10. (Original) The method of claim 9, wherein verifying the access-request message comprises:

temporarily storing the authenticator value written in the authenticator field of the received access-request message;

replacing the authenticator value with a prescribed value in the authenticator field, the prescribed value being previously defined between the message transmitter and the message receiver to form a verification access-request message;

performing an encrypting algorithm using the verification access-request message and the shared secret key to form a message digest; and

comparing the message digest with the temporarily stored authenticator value, wherein the access-request message is verified if the message digest and the authenticator value are identical to each other, and wherein the access-request message is abnormal if the message digest and the authenticator value are not identical to each other.

11. (Previously Presented) The method of claim 9, wherein performing user authentication comprises:

decrypting the encrypted user password written in an attribute field of the processed access-request message using the temporary authenticator value of the processed access-request message;

comparing the decrypted user password and a user password stored in a database;

determining that the user authentication is successful if the decrypted user password and the stored user password are identical to each other; and

determining that the user authentication has failed if the decrypted user password and the stored user password are not identical to each other.

12. (Original) The method of claim 9, wherein transmitting the access-request message comprises:

encrypting a user password using the temporary authenticator value;

creating the authenticator value for authentication of the access-request message using the temporary authenticator value and a prescribed value previously defined between the message transmitter and the message receiver; and

writing the authenticator value in the authenticator field and generating the access-request message.

13. (Currently Amended) The method of claim 12, wherein encrypting the user password comprises:

generating an arbitrary value which is ~~differently~~ arbitrarily created each time a message is generated as a temporary authenticator value;

writing the temporary authenticator value in the attribute field of the access-request message; and

encrypting the user password using the temporary authenticator value and the shared secret key.

14. (Original) The method of claim 12, wherein generating the authenticator value comprises:

forming the access-request message by filling attribute fields of the access-request message with the temporary authenticator value and the encrypted user password, and filling the authenticator field with the prescribed value;

executing an encryption algorithm using the generated access-request message and the shared secret key to form a message digest; and

taking the message digest as the authenticator value.

15. (Currently Amended) The method of claim 12, wherein the temporary ~~authentication~~ authenticator value is randomly generated each time a new access-request message is generated, such that the temporary authenticator value is not known beforehand.

16. (Original) The method of claim 9, wherein the message transmitter is a Foreign Agent (FA) and wherein the message receiver is an Authentication, Authorization, and Accounting (AAA) server.

17. (Original) A method of processing an access-request message, comprising:

receiving an access-request message having a code field, an identifier field, a length field, and authenticator value, and at least one attribute field, the authenticator value being a message digest created by encrypting a temporary access-request message, and the at least one attribute field including an encrypted user password;

processing the authenticator value to determine if the access-request message is a valid access-request message or an abnormal access-request message; and

performing user authentication if it is determined that the access-request message is a valid access-request message and discarding the access-request message if it is determined that the access-request message is abnormal.

18. (Original) The method of claim 17, wherein the access-request message is formed by writing a temporary randomly generated authenticator value in a first attribute field of a temporary access-request message, writing a prescribed value into an authenticator field of the temporary access-request message and writing the encrypted password into a second attribute field, encrypting the user password using the temporary authenticator value, executing an encryption algorithm on the temporary access-request message to form a message digest, replacing the temporary authenticator value of the temporary access-request message with the message digest to form the access-request message.

19. (Original) The method of claim 17, wherein processing the authenticator value comprises:

temporarily storing the authenticator value written in the authenticator field of the received access-request message;

replacing the authenticator value with a prescribed value in the authenticator field to form a verification access-request message, the prescribed value being previously defined between the message transmitter and the message receiver;

performing an encrypting algorithm using the verification access-request message and a shared secret key to form a message digest; and

comparing the message digest with the temporarily stored authenticator value, wherein the access-request message is verified if the message digest and the authenticator value are identical to each other, and wherein the access-request message is abnormal if the message digest and the authenticator value are not identical to each other.

20. (Previously Presented) An improved method of processing an access-request message at a message receiving point, the improvement comprising authenticating the access-request message prior to performing user authentication of the access-request message such that abnormal access-request messages are not processed for user authentication,

wherein authenticating the access-request message comprises:

temporarily storing contents of an authenticator field of the access-request message;

filling the authenticator field with a prescribed value known to each of a message origination point and the message receiving point to form a temporary access-request message;

performing an encrypting algorithm on the temporary access-request message to obtain a message digest; and

verifying the access-request message by comparing the temporarily stored authenticator value to the message digest.

21. (Canceled)

22. (Previously Presented) The improvement of claim 20, wherein verifying the access-request message comprises determining the access-request message to be normal if the authenticator value and the message digest are identical to each other, and determining the access-request message to be abnormal if the authenticator value and the message digest are not identical to each other.

23. (Original) The method of claim 22, wherein if the access-request message is determined to be abnormal based on the authentication procedure, the access-request message is discarded, and wherein if the access-request message is determined to be normal, the message is processed for user authentication.

24.-27. (Canceled)